FORM-PTO-1390 (Rev. 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371**	ATTORNEY'S DOCKET NUMBER 032326-168 U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5) 09/937397

INTERNATIONAL APPLICATION NO. PCT/FR00/00723	INTERNATIONAL FILING DATE March 22, 2000	PRIORITY DATE CLAIMED March 26, 1999

TITLE OF INVENTION
COUNTERMEASURE METHOD IN AN ELECTRIC COMPONENT IMPLEMENTING AN ELLIPTICAL CURVE TYPE PUBLIC KEY CRYPTOGRAPHY ALGORITHM

APPLICANT(S) FOR DO/EO/US
Jean-Sébastien CORON

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   - b. ☒ has been transmitted by the International Bureau.
   - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   - b. ☐ have been transmitted by the International Bureau.
   - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   - d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.50) 09/937397	INTERNATIONAL APPLICATION NO. PCT/F00/00723	ATTORNEY'S DOCKET NUMBER 032326-168

17. □ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)): *Neither international preliminary* examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO .... $1,000.00 (960) International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO .... $860.00 (970) International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO .... $710.00 (958) International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) .... $690.00 (956) International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00 (962)		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 □ 30 □ months from the earliest claimed priority date (37 CFR 1.492(e)).	$ -0-	

Claims	Number Filed	Number Extra	Rate		
Total Claims	15 -20 =	-0-	X$18.00 (966)	$ -0-	
Independent Claims	3 -3 =	-0-	X$80.00 (964)	$ -0-	
Multiple dependent claim(s) (if applicable)			+$270.00 (968)	$ -0-	

TOTAL OF ABOVE CALCULATIONS =	$ 860.00	
Reduction for 1/2 for filing by small entity, if applicable (see below).	$ -0-	-
SUBTOTAL =	$ 860.00	
Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 □ 30 □ months from the earliest claimed priority date (37 CFR 1.492(f)). +	$ -0-	
TOTAL NATIONAL FEE =	$ 860.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property +	$ -0-	
TOTAL FEES ENCLOSED =	$ 860.00	
	Amount to be: refunded	$
	charged	$

a. □ Small entity status is hereby claimed.

b. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

c. □ Please charge my Deposit Account No. 02-4800 in the amount of $______ to cover the above fees. A duplicate copy of this sheet is enclosed.

d. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

James LaBarre
SIGNATURE

James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

Patent
Attorney's Docket No. 032326-168

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Jean-Sébastien CORON	Group Art Unit: Unassigned
Application No.: Unassigned	Examiner: Unassigned
Filed: September 26, 2001	
For: COUNTERMEASURE METHOD IN AN ELECTRIC COMPONENT IMPLEMENTING AN ELLIPTICAL CURVE TYPE PUBLIC KEY CRYPTOGRAPHY ALGORITHM	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

IN THE SPECIFICATION:

Page 1, immediately following the title appearing on lines 1-3, insert the following:

--This disclosure is based upon French Application No. 99/03920, filed on March 26, 1999 and International Application No. PCT/FR00/00723, filed March 22, 2000, which was published on October 5, 2000 in a language other than English, the contents of which are incorporated herein by reference.

Background of the Invention--

Page 11, before line 3, insert the following heading:

--**Description of the Invention**--

Add the following Abstract:

--A countermeasure method in an electronic component implementing an elliptical curve based public key cryptography algorithm. A new decryption integer d' is calculated such that the decryption of an encrypted message on the basis of a private key d and the number of points n of an elliptical curve provides the same result with d' as with d, by performing the operation Q=d*P, whereby P is a point of the curve. Four steps are employed in the calculation: 1) a security parameter s is determined, 2) a random number k ranging from 0-2^s is drawn, 3) the integer d'=d+k*n is calculated, and 4) Q=d'.P is calculated.--

IN THE CLAIMS:

Kindly replace claims 1-15, as follows.

1. (Amended) A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves in which a deciphering integer d' is calculated, using a private key d and a number of points n on an elliptical curve, such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d', gives the same result as with d, by effecting the operation Q=d*P, where P is a point on the curve, said method including the following steps:

1) determining a security parameter s;

2) drawing a random number k between 0 and 2^s;

3) calculating the integer d'=d+k*n; and

4) calculating Q=d'*P.

2. (Amended) A countermeasure method according to Claim 1, wherein a new deciphering integer d' is calculated at each new execution of the deciphering algorithm.

3. (Amended) A countermeasure method according to Claim 1, further including the step of incrementing a counter at each new execution of the deciphering algorithm until a fixed value T is reached.

4. (Amended) A countermeasure method according to Claim 3, wherein, once the value T has been reached, a new deciphering integer is calculated and the counter is reset to zero.

5. (Amended) A countermeasure method according to Claim 3, wherein the value T is equal to the integer 16.

6. (Amended) A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves defined on a finite field GF(p), where p is a prime number, according to the equation $y^2=x^3+ax+b$ and where a random calculation modulus of the form p'=p*r, where r is a

random integer, is used at each new execution of the algorithm, said method including the execution of a scalar multiplication operation according to the following steps:

1) determining a security parameter s;

2) drawing a random number r whose binary representation comprises s bits;

3) calculating p'=p*r;

4) executing the scalar multiplication operation Q=d.P, where P is a point on a curve, and said operation is performed modulo p'; and

5) performing the reduction operation modulo p of the coordinates of the point Q.

7. (Amended) A countermeasure method according to Claim 6, wherein a new integer is calculated at each new execution of the cryptography algorithm.

8. (Amended) A countermeasure method according to Claim 6, further including the step of incrementing a counter at each new execution of the cryptography algorithm.

9. (Amended) A countermeasure method according to Claim 8, wherein the counter is reset to zero when it has reached a value T.

10. (Amended) A countermeasure method according to Claim 9, wherein the value T is equal to sixteen.

11. (Amended) A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves in which a new deciphering key d' is calculated, using the private key d and a number of points n on an elliptical curve, such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d', gives the same result as with d, by performing the operation Q=d*P, where P is a point on the curve to which a scalar multiplication algorithm is applied, said method comprising the following steps:

1) drawing a random point R on the curve;

2) calculating P'=P+R;

3) performing the scalar multiplication operation Q'=d.P';

4) performing the scalar multiplication operation S=d.R; and

5) calculating Q=Q' - S.

12. (Amended) A countermeasure method according to Claim 11, further including the step of incrementing a counter at each new execution of the deciphering algorithm up to a value T.

13. (Amended) A countermeasure method according to Claim 12, wherein the counter is reset to zero once the value T has been reached.

14. (Amended) A countermeasure method according to Claim 11, wherein the elliptical curve has two points such that S=d*R, and wherein steps 1 and 4 are replaced by the following steps 1' and 4':

1') Replacing R with 2.R.

4') Replacing S with 2.S.

15. (Amended) A countermeasure method according to Claim 14, further including the step of incrementing a counter at each new execution of the deciphering algorithm up to a value T.

REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: James LaBarre
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: September 26, 2001

Attachment to Preliminary Amendment dated September 26, 2001

Marked-up Claims 1-15

1. (Amended) A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves [consisting in calculating] in which a deciphering integer d' is calculated, using [the] a private key d and [the] a number of points n on [the said] an elliptical curve, [a new deciphering integer d'] such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d', gives the same result as with d, by effecting the operation Q=d*P, [P being] where P is a point on the curve, [a method characterised in that it comprises four] said method including the following steps:

1) determining a security parameter s; [in practice s can be taken close to 30.]

2) drawing a random number k between 0 and [2^s.] 2^s;

3) calculating the integer d'=d+k*n[.]; and

4) calculating [Q=d'.P] Q=d'*P.

2. (Amended) A countermeasure method according to Claim 1, [characterised in that a first variant consists of the fact that] wherein a new deciphering integer d' is calculated at each new execution of the deciphering algorithm.

3. (Amended) A countermeasure method according to Claim 1, [characterised in that a second variant consists of the fact that a counter is incremented] further including

Attachment to Preliminary Amendment dated September 26, 2001

Marked-up Claims 1-15

the step of incrementing a counter at each new execution of the deciphering algorithm until a fixed value T is reached.

4. (Amended) A countermeasure method according to Claim 3, [characterised in that] wherein, once the value T has been reached, a new [enciphering] deciphering integer is calculated [according to the method of Claim 1] and the counter is reset to zero.

5. (Amended) A countermeasure method according to Claim 3, [characterised in that] wherein the value T is equal to the integer 16.

6. (Amended) A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves defined on a finite field GF(p), where p [being] is a prime number, [having as its equation y^2=x^3+ax+b, consisting in using] according to the equation $y^2=x^3+ax+b$ and where a random calculation modulus [at each new execution] of the form p'=p*r, where r is a random integer is used at each new execution of the algorithm [and having a point P, characterised in that the] said method [executes the] including the execution of a scalar multiplication operation [in five] according to the following steps:

1) determining a security parameter s; [in practice, s can be taken to be close to the number 60.]

Attachment to Preliminary Amendment dated September 26, 2001

Marked-up Claims 1-15

2) drawing [the] a random number r whose binary representation [makes] comprises s bits[.];

3) calculating p'=p*r[.];

4) executing the scalar multiplication operation Q=d.P, [the operations being] where P is a point on a curve, and said operation is performed modulo p'[.]; and

5) performing the reduction operation modulo p of the coordinates of the point Q.

7. (Amended) A countermeasure method according to Claim 6, [characterised in that] wherein a new integer is calculated at each new execution of the [deciphering] cryptography algorithm.

8. (Amended) A countermeasure method according to Claim 6, [characterised in that] further including the step of incrementing a counter [is incremented] at each new execution of the [deciphering] cryptography algorithm.

9. (Amended) A countermeasure method according to Claim 8, [characterised in that] wherein the counter is reset to zero when it has reached a value T.

Attachment to Preliminary Amendment dated September 26, 2001

Marked-up Claims 1-15

10. (Amended) A countermeasure method according to [Claim 8 or] Claim 9, [characterised in that] wherein the value T is equal to sixteen.

11. (Amended) A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves [consisting in calculating] in which a new deciphering key d' is calculated, using the private key d and [the] a number of points n on [the said] an elliptical curve, [a new deciphering integer d'] such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d', gives the same result as with d, by performing the operation Q=d*P, where P [being] is a point on the curve to which [the] a scalar multiplication algorithm is applied, [adding to it a random point R by an integer d according to the equation Q=d*P, a method characterised in that it comprises] said method comprising the following [five] steps:

1) drawing a random point R on the curve[.];
2) calculating P'=P+R[.];
3) performing the scalar multiplication operation Q'=d.P'[.];
4) performing the scalar multiplication operation S=d.R[.]; and
5) calculating Q=Q' - S.

Attachment to Preliminary Amendment dated September 26, 2001

Marked-up Claims 1-15

12. (Amended) A countermeasure method according to Claim [12, characterised in that] 11, further including the step of incrementing a counter [is incremented] at each new execution of the deciphering algorithm up to a value T.

13. (Amended) A countermeasure method according to Claim 12, [characterised in that] wherein the counter is reset to zero once the value T has been reached.

14. (Amended) A countermeasure method according to Claim 11, [characterised in that] wherein the elliptical curve has [in memory] two points such that S=d*R, and wherein steps 1 and 4 [then being] are replaced by the following steps 1' and 4':

1') Replacing R with 2.R.

4') Replacing S with 2.S.

15. (Amended) A countermeasure method according to Claim 14, [characterised in that] further including the step of incrementing a counter [is incremented] at each new execution of the deciphering algorithm up to a value T.

A COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT IMPLEMENTING A ELLIPTICAL CURVE TYPE PUBLIC KEY CRYPTOGRAPHY ALGORITHM

The present invention relates to a countermeasure method in an electronic component implementing an elliptical curve type public key cryptography algorithm.

In the conventional model of secret key cryptography, two persons wishing to communicate by means of a non-secure channel must first agree on a secret enciphering key K. The enciphering function and the deciphering function implement the same key K. The drawback of the secret key enciphering system is that the said system requires the prior communication of the key K between the two persons by means of a secure channel, before any enciphered message is sent over the non-secure channel. In practice, it is generally difficult to find a perfectly secure communication channel, particularly if the distance separating the two persons is great. Secure channel means a channel for which it is impossible to know or modify the information passing over the said channel. Such a secure channel can be accomplished by means of a cable connecting two terminals, possessed by the said two persons.

The concept of public key cryptography was invented by Whitfield Diffie and Martin Hellman in 1976. Public key cryptography makes it possible to resolve the problem of the distribution of the keys over a non-secure channel. The principle of public key cryptography consists in using a pair of keys, a public enciphering key and a private deciphering key. It must be unfeasible from the calculation point of view to find the private deciphering key from the public enciphering key. A person A wishing to communicate information to a person B uses the public enciphering key of the person B. Only the person B possesses the private key associated with his public key. Only the person B is therefore capable of deciphering the message sent to him.

Another advantage of public key cryptography over secret key cryptography is that public key cryptography allows authentication by the use of an electronic signature.

The first embodiment of the public key enciphering scheme was developed in 1977 by Rivest, Shamir and Adleman, who invented the RSA enciphering system. RSA security is based on the difficulty of factorising a large number which is the product of two prime numbers.

Since then, many public key enciphering systems have been proposed, the security of which is based on different calculatory problems (this list is not exhaustive):

- Merckle-Hellman backpack:

This enciphering system is based on the difficulty of the problem of the sum of subsets.

- McEliece:

This enciphering system is based on the theory of algebraic codes. It is based on the problem of the decoding of linear codes.

- El Gamal:

This enciphering system is based on the difficulty of the discrete logarithm in a finite field.

- Elliptical curves:

The elliptical curve enciphering system constitutes a modification to existing cryptographic systems in order to apply them to the field of elliptical curves.

The use of elliptical curves in cryptographic systems was proposed independently by Victor Miller and Neal Koblitz in 1985. Actual applications of elliptical curves were envisaged early in the 1990s.

The advantage of cryptosystems based on elliptical curves is that they provide security equivalent to other cryptosystems but with smaller key sizes. This saving in key size entails a decrease in memory requirements and a reduction in calculation times, which makes the use of elliptical curves particularly suitable for applications of the smart card type.

An elliptical curve on a finite field GF(q^n) (q being a prime number and n an integer) is the set of points (x,y) with x the X-axis and y the Y-axis belonging to GF(q^n) the solution to the equation:

y^2=x^3+ax+b
if q is greater than or equal to 3 and
y^2+x*y=x^3+a*x^2+b
if q=2.

The two classes of elliptical curves which are most used in cryptography are the following classes:

1) Curves defined on the finite field GF(p) (the set of integers modulo p, p being a prime number) having as its equation:
y^2=x^3+ax=b
2) Elliptic curves on the finite field GF(2^n) having as its equation y^2+xy=x^3+ax^2+b

For each of these two classes of curves, an operation of addition of points is defined: given two points P and Q, the sum R=P+Q is a point on the curve, the coordinates of which are expressed by means of the coordinates of the points P and Q in accordance with formulae whose expression is given in the work

"Elliptic Curve Public Key Cryptosystem" by Alfred J Menezes.

This addition operation makes it possible to define a scalar multiplication operation: given a point P belonging to an elliptical curve and an integer d, the result of the scalar multiplication of P by a point d such that Q=d.P=P+PP....+P d times.

The security of cryptography algorithms on elliptical curves is based on the difficulty of the discrete logarithm on elliptical curves, the said problem consisting, using two points Q and P belonging to an elliptical curve E, in finding, if such exists, an integer x such that Q=x.P.

There are many cryptographic algorithms based on the problem of the discrete logarithm.

These algorithms are easily transposable to elliptical curves. Thus it is possible to use algorithms providing authentication, confidentiality, integrity check and key exchange.

A point common to the majority of cryptographic algorithms based on elliptical curves is that they comprise as a parameter an elliptical curve defined on a finite field and a point P belonging to this elliptical curve. The private key is an integer d chosen randomly. The public key is a point on the curve Q such that Q=d.P. These cryptographic algorithms generally involve a scalar multiplication in the calculation of a point R=d.T, where d is the secret key.

These algorithms are easily transposable to elliptical curves. Thus it is possible to use algorithms providing authentication, confidentiality, integrity check and key exchange.

A point common to the majority of cryptographic algorithms based on elliptical curves is that they comprise as a parameter an elliptical curve defined on a finite field and a point P belonging to this elliptical curve. The private key is an integer d chosen randomly. The public key is a point on the curve Q such that Q=d.P. These cryptographic algorithms generally involve a scalar multiplication in the calculation of a point R=d.T, where d is the secret key.

In this section, an enciphering algorithm based on an elliptical curve is described. A document Menkus B: "Two important data encryption structures reported broken in record times" EDPACS, Jan. 1999, Auerbach Publications, USA, Vol. 26, N° 7, pages 15-18, XP000884687 ISSN: 0736-6981, cited D2, suggests the utilisation of random numbers without specifying the implementing of these random numbers in the context of an elliptical curve algorithm. The scheme of this algorithm is similar to the El Gamal enciphering scheme. A message m is enciphered as follows:

The cipher clerk chooses an integer k randomly and calculates the points k.P=(x1,y1) and k.Q=(x2,y2) on the curve, and the integer c= x2 + m. The cipher of m is the triplet (x1,y1,c).

The deciphering clerk, who possesses d, deciphers m by calculating:

(x'2,y'2)=d(x1,y1) and m=c-x'2

In order to effect the scalar multiplications necessary in the calculation methods described previously, several algorithms exist:

"Double and add" algorithm;

"Addition-subtraction" algorithm;

Algorithm with addition chains;

Algorithm with window;

Algorithm with signed representation.

This list is not exhaustive. The simplest algorithm and the one which is most used is the "double and add" algorithm. The "double and add" algorithm takes as its input a point P belonging to a given elliptical curve and an integer d. The integer d is denoted d=(d(t),d(t-1),…,d(0)), where (d(t),d(t-1),…,d(0)) is the binary representation of d, with d(t) the most significant bit and d(0) the least significant bit. The algorithm returns as an output the point Q=d.P.

The "double and add" algorithm includes the following three steps:

```
1) Initialising the point Q with the value P
2) For i ranging from t-1 to 0, executing:
    2a) Replacing Q with 2Q
    2b) If d(i)=1 replacing Q with Q+P
```

3) Returning Q.

It became clear that the implementation of a public key enciphering algorithm of the elliptical curve type on a smart card was vulnerable to attacks consisting of a differential analysis of current consumption making it possible to find the private deciphering key. These attacks are known as DPA attacks, the acronym for Differential Power Analysis. The principle of these DPA attacks is based on the fact that the current consumption of the microprocessor executing the instructions varies according to the data item being manipulated.

In particular, when an instruction is manipulating a data item in which a particular bit is constant, where the value of the other bits may vary, analysis of the current consumption related to the instruction shows that the mean consumption of the instruction is not the same according to whether the particular bit takes the value 0 or 1. The attack of the DPA type therefore makes it possible to obtain additional information on the intermediate data manipulated by the microprocessor of the card when a cryptographic algorithm is being executed. This additional information can in some cases reveal the private parameters of the deciphering algorithm, making the cryptographic system insecure.

In the remainder of this document a description is given of a method of DPA attack on an algorithm of the elliptical curve type performing an operation of the type consisting of the scalar multiplication of a point P by an integer d, the integer d being the secret key. This attack directly reveals the secret key d. It therefore seriously compromises the security of the implementation of elliptical curves on a smart card.

The document Paul Kocher et al: "Introduction to Differential Power Analysis and Related Attacks" <URL: http://www.cryptography.com/dpa/technical/index.html>, pages 1-8, XP002132318 San Francisco, CA, USA, cited D1, suggests the utilisation of counterattacks in implementations of the Diffie-Hellman, RSA and DSS type and other systems without ever proposing precise implementations.

The first step of the attack is the recording of the current consumption corresponding to the execution of the "double and add" algorithm described previously for N distinct points P(1),…, P(N). In an algorithm based on elliptical curves, the microprocessor of the smart card will perform N scalar multiplications d.P(1),…,d.P(N).

For clarity of the description of the attack, the first step is to describe a method for obtaining the value of the bit d(t-1) of the secret key d, where (d(t),d(t-1),…,d(0)) is the binary representation of d, with d(t) the most significant bit and d(0) the least significant bit. Next the description of an algorithm which makes it possible to find the value of d is given.

The points P(1) to P(N) are grouped together according to the value of the last bit of the abscissa of 4.P, where P designates one of the points P(1) to P(N). The first group consists of the points P such that the last bit of the abscissa of 4.P is equal to 1. The second group consists of the points P such that the last bit of the abscissa of 4.P is equal to 0. The mean of the current consumptions corresponding to each of the two groups is calculated, and the difference curve between these two means is calculated.

If the bit d(t-1) of d is equal to 0, then the scalar multiplication algorithm previously described calculates and stores in memory the value of 4.P. This means that, when the algorithm is executed in a smart card, the microprocessor of the card will actually calculate 4.P. In this case, in the first message group, the last bit of the data item manipulated by the microprocessor is always at 1, and in the second message group the last bit of the data item manipulated is always at 0. The mean of the current consumptions corresponding to each group is therefore different. There therefore appears, in the difference curve between the two means, a differential current consumption peak.

If on the other hand the bit d(t-1) of d is equal to 1, the exponentiation algorithm described previously does not calculate the point 4.P. When the algorithm is executed by the smart card, the microprocessor therefore never manipulates the data item 4.P. Therefore no differential consumption peak appears.

This method therefore makes it possible to determine the value of the bit d(t-1) of d.

The algorithm described in the following section is a generalisation of the previous algorithm. It makes it possible to determine the value of the secret key d:

The input is defined by N points denoted P(1) to P(N) corresponding to N calculations performed by the smart card, and the output by an integer h.

The said algorithm is implemented as follows in three steps.

```
1) Executing h=1;
2) For i ranging from t-1 to 1, executing:
    2)1) Classifying the points P(1) to P(N) according to the value of the last bit of the abscissa of (4*h).P;
    2)2) Calculating the current consumption mean for each of the two groups;
    2)3) Calculating the difference between the two means;
    2)4) If the difference shows a differential consumption peak, doing h=h*2; otherwise doing h=h*2+1;
3) Returning h.
```

The above algorithm supplies an integer h such that d=2*h or d=2*h+1. In order to obtain the value of d, it then suffices to test the two possible hypotheses.

The attack of the DPA type described therefore makes it possible to find the private key d.

The method of the invention consists in the devising of three countermeasures to guard against the DPA attack described above.

The method of the first countermeasure consists in calculating, from the private key d and the number of points N on the elliptical curve, a new deciphering integer d', such that the deciphering of any enciphered message with d' gives the same result as with d.

In the case of a cryptographic algorithm based on the use of elliptical curves effecting the operation $Q=d.P$ where d is the private key and P a point on the curve, the calculation of $Q=d.P$ is replaced by the following method in four steps:

1) Determining a security parameter s; in practice s can be taken close to 30.

2) Drawing a random number k between 0 and 2^s.

3) Calculating the integer $d'=d+k*n$.

4) Calculating $Q=d'.P$.

The method of the first countermeasure comprises two variants which relate to the updating of the integer d'. The first variant consists of the fact that a new deciphering integer d' is calculated at each new execution of the deciphering algorithm, according to the method described previously. The second variant consists of the fact that a counter is incremented at each new execution of the deciphering algorithm. When this counter reaches a fixed value T, a new deciphering integer d' is calculated according to the method described previously, and the counter is reset to zero. In practice, T=16 can be taken.

The method of the first countermeasure therefore makes the previously described DPA attack impossible by changing the deciphering integer d.

The method of the second countermeasure applies to the first class of curves previously described, that is to say the curves defined on the finite field GF(p) having as its equation y^2=x^3+ax+b. The method of the second countermeasure consists in using a random calculation modulus at each new execution. This random modulus is of the form p' = p*r where r is a random integer. The scalar multiplication operation Q=d.P effected in an algorithm based on an elliptical curve is then effected according to the following method in five steps:

1) Determining a security parameter s; in practice, s can be taken to be close to the number 60.

2) Drawing the random number r whose binary representation makes s bits.

3) Calculating p'=p*r.

4) Executing the scalar multiplication operation Q=d.P, the operations being performed modulo p'.

5) Performing the reduction operation modulo p of the coordinates of the point Q.

The method of the second countermeasure comprises two variants which relate to the updating of the integer r. The first variant consists of the fact that a new integer r is calculated at each new execution of the deciphering algorithm, according to the method described previously. The second variant consists of the fact that a counter is incremented at each new execution of the deciphering algorithm. When this counter reaches a fixed value T, a new integer r is calculated according to the method described previously, and the counter is reset to zero. In practice, T+16 can be taken.

The method of the third countermeasure consists in "masking" the point P to which it is wished to apply the scalar multiplication algorithm by adding a random point R to it.

The method of scalar multiplication of a point P by an integer d according to Q=d.P comprises the following five steps:

1) Drawing a random point R on the curve.
2) Calculating P'=P+R.
3) Scalar multiplication operation Q'=d.P'.
4) Scalar multiplication operation S=d.R.
5) Calculating Q=Q' - S.

The method of the third countermeasure comprises three variants. The first variant consists of the fact that a counter is incremented at each new execution of the deciphering algorithm. When the deciphering algorithm is first executed, the algorithm is executed according to the five-step method described above. As long as the counter has not reached the limit value T, steps 1 and 4 of the method described above are not executed, the points R and S keeping the values taken during the previous execution. When the counter reaches the limit value T, the deciphering algorithm is implemented according to the method described previously in five steps, and the counter is reset to zero. In practice, T=16 can be taken.

The second variant consists of the fact that the card initially has in memory two points on the elliptical curves such that S=d.R. Steps 1 and 4 of the previous deciphering algorithm are replaced by the following steps 1′ and 4′:

1′) Replacing R with 2.R.

4′) Replacing S with 2.S.

The third variant consists of a modification of the second variant characterised in that a counter is incremented at each new execution of the deciphering algorithm. When the deciphering algorithm is first executed, the algorithm is executed according to the five-step method of the second variant described above. As long as the counter has not reached a limit value T, steps 1′ and 4′ of the method described above are not executed, points r and S keeping the values taken during the previous execution. When the counter reaches a limit value T, the deciphering algorithm is implemented according to the method previously described in five steps, and the counter is reset to zero. In practice, T=16 can be taken.

The application of the above three countermeasure methods makes it possible to protect any cryptographic algorithm based on elliptical curves against the DPA attack described above. The three countermeasures presented are also compatible with each other: it is possible to apply to the RSA deciphering algorithm one, two or three of the countermeasures described.

CLAIMS

1. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves consisting in calculating, using the private key d and the number of points n on the said elliptical curve, a new deciphering integer d′ such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d′, gives the same result as with d, by performing the operation Q=d*P, P being a point on the curve, a method characterised in that it comprises four steps:

1) Determining a security parameter s; in practice s can be taken close to 30.

2) Drawing a random number k between 0 and 2^s.

3) Calculating the integer d′=d+k*n.

4) Calculating Q=d′.P.

2. A countermeasure method according to Claim 1, characterised in that a first variant consists of the fact that a new deciphering integer d′ is calculated at each new execution of the deciphering algorithm.

3. A countermeasure method according to Claim 1, characterised in that a second variant consists of the fact that a counter is incremented at each new execution of the deciphering algorithm until a fixed value T is reached.

4. A countermeasure method according to Claim 3, characterised in that, once the value T has been reached, a new enciphering integer is calculated according to the method of Claim 1 and the counter is reset to zero.

5. A countermeasure method according to Claim 3, characterised in that the value T is equal to the integer 16.

6. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves defined on a finite field GF(p), p being a prime number, having as its equation y^2=x^3+ax+b, consisting in using a random calculation modulus at each new execution of the form p'=p*r where r is a random integer and having a point P, characterised in that the said method executes the scalar multiplication operation in five steps:

1) Determining a security parameter s; in practice, s can be taken to be close to the number 60.

2) Drawing the random number r whose binary representation makes s bits.

3) Calculating p'=p*r.

4) Executing the scalar multiplication operation Q=d.P, the operations being performed modulo p'.

5) Performing the reduction operation modulo p of the coordinates of the point Q.

7. A countermeasure method according to Claim 6, characterised in that a new integer is calculated at each new execution of the deciphering algorithm.

8. A countermeasure method according to Claim 6, characterised in that a counter is incremented at each new execution of the deciphering algorithm.

9. A countermeasure method according to Claim 8, characterised in that the counter is reset to zero when it has reached a value T.

10. A countermeasure method according to Claim 8 or Claim 9, characterised in that the value T is equal to sixteen.

11. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves consisting in calculating, using the private key d and the number of points n on the said elliptical curve, a new deciphering integer d' such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d', gives the same result as with d, by performing the operation $Q=d*P$, P being a point on the curve to which the scalar multiplication algorithm is applied, adding to it a random point R by an integer d according to the equation $Q=d*P$, a method characterised in that it comprises the following five steps:

1) Drawing a random point R on the curve.
2) Calculating $P'=P+R$.
3) Scalar multiplication operation $Q'=d.P'$.
4) Scalar multiplication operation $S=d.R$.

5) Calculating Q=Q′ - S.

12. A countermeasure method according to Claim 11, characterised in that a counter is incremented at each new execution of the deciphering algorithm up to a value T.

13. A countermeasure method according to Claim 12, characterised in that the counter is reset to zero once the value T has been reached.

14. A countermeasure method according to Claim 11, characterised in that the elliptical curve has in memory two points such that S=d*R, steps 1 and 4 then being replaced by steps 1′ and 4′:

1′) Replacing R with 2.R.
4′) Replacing S with 2.S.

15. A countermeasure method according to Claim 14, characterised in that a counter is incremented at each new execution of the deciphering algorithm up to a value T.

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY **(Includes Reference to Provisional and International (PCT) Applications)**	Attorney's Docket No. 032326-168

As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name;
I BELIEVE I AM THE ORIGINAL, FIRST AND SOLE INVENTOR (IF ONLY ONE NAME IS LISTED BELOW) OR AN ORIGINAL, FIRST AND JOINT INVENTOR (IF PLURAL NAMES ARE LISTED BELOW) OF THE SUBJECT MATTER WHICH IS CLAIMED AND FOR WHICH A PATENT IS SOUGHT ON THE INVENTION ENTITLED:

A COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT IMPLEMENTING A ELLIPTICAL CURVE TYPE PUBLIC KEY CRYPTOGRAPHY ALGORITHM

The specification of which (check only one item below):

□ is attached hereto.

□ was filed as United States Patent Application Number ________
on __________
and was amended on _______ (if applicable).

☒ was filed as International (PCT) Application Number **PCT/FR00/00723**
on **March 22, 2000**
and was amended on _______ (if applicable).

I HAVE REVIEWED AND UNDERSTAND THE CONTENTS OF THE ABOVE-IDENTIFIED SPECIFICATION, INCLUDING THE CLAIMS, AS AMENDED BY ANY AMENDMENT REFERRED TO ABOVE.

I ACKNOWLEDGE THE DUTY TO DISCLOSE TO THE U.S. PATENT AND TRADEMARK OFFICE ALL INFORMATION KNOWN TO ME TO BE MATERIAL TO PATENTABILITY AS DEFINED IN TITLE 37, CODE OF FEDERAL REGULATIONS, Sec. 1.56 (as amended effective March 16, 1992);

I do not know and do not believe the said invention was ever known or used in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to said application; that said invention was not in public use or on sale in the United States of America more than one year prior to said application; that said invention has not been patented or made the subject of an inventor's certificate issued before the date of said application in any country foreign to the United States of America on any application filed by me or my legal representatives or assigns more than six months prior to said application;

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any International (PCT) Application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT International (PCT) Application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §119:

COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. §119
FRANCE	99/03920	March 26, 1999	☒Yes □No
			□Yes □No
			□Yes □No
			□Yes □No
			□Yes □No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

________ (APPLICATION NUMBER) ________ (FILING DATE)

________ (APPLICATION NUMBER) ________ (FILING DATE)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D)
(Includes Reference to Provisional and International (PCT) Applications)

Attorney's Docket
No. 032326-168

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States applications(s) or International (PCT) Application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations § 1.56, which became available between the filing date of the prior application(s) and the national or international filing date of this application:

PRIOR U.S. APPLICATIONS OR INTERNATIONAL (PCT) APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. § 120:

U.S. APPLICATIONS			STATUS *(check one)*		
U.S. APPLICATION NUMBER	U.S. FILING DATE		PATENTED	PENDING	ABANDONED
			□	□	□
PCT APPLICATIONS DESIGNATING THE U.S.					
PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (if any)			
PCT/FR00/00723	March 22, 2000				

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the U.S. Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	R. Danny Huntington	27,903	Gerald F. Swiss	30,113
Robert S. Swecker	19,885	Eric H. Weisblatt	30,505	Charles F. Wieland III	33,096
Platon N. Mandros	22,124	James W. Peterson	26,057	Bruce T. Wieder	33,815
Benton S. Duffett, Jr.	22,030	Teresa Stanek Rea	30,427	Todd R. Walters	34,040
Norman H. Stepno	22,716	Robert E. Krebs	25,885	Ronni S. Jillions	31,979
Ronald L. Grudziecki	24,970	William C. Rowland	30,888	Harold R. Brown III	36,341
Frederick G. Michaud, Jr.	26,003	T. Gene Dillahunty	25,423	Allen R. Baum	36,086
Alan E. Kopecki	25,813	Patrick C. Keane	32,858	Steven M. duBois	35,023
Regis E. Slutter	26,999	B. Jefferson Boggs, Jr.	32,344	Brian P. O'Shaughnessy	32,747
Samuel C. Miller, III	27,360	William H. Benz	25,952	Kenneth B. Leffler	36,075
Robert G. Mukai	28,531	Peter K. Skiff	31,917	Fred W. Hathaway	32,236
George A. Hovanec, Jr.	28,223	Richard J. McGrath	29,195		
James A. LaBarre	28,632	Matthew L. Schneider	32,814		
E. Joseph Gess	28,510	Michael G. Savage	32,596		

21839

and: ______________________________.

Address all correspondence to:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

21839

Address all telephone calls to: James A. LaBarre at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) **(Includes Reference to Provisional and International (PCT) Applications)**	Attorney's Docket No. 032326-168

1-00

FULL NAME OF SOLE OR FIRST INVENTOR CORON Jean-Sébastien	SIGNATURE	DATE 9/10/2007
RESIDENCE (CITY & STATE/COUNTRY) 4 rue Léon Delagrange – 75015 PARIS - FRANCE JRX		CITIZENSHIP FRANCE
POST OFFICE ADDRESS (HOME ADDRESS) 4 rue Léon Delagrange – 75015 PARIS - FRANCE		
FULL NAME OF SECOND JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF THIRD JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF NINTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS)		
FULL NAME OF TENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		